Using Blockchain Analysis From Investigation to Trial

C. Alden Pelker
Senior Counsel
Computer Crime & Intellectual Property Section

Christopher B. Brown
Assistant United States Attorney
District of Columbia

Richard M. Tucker
Senior Vice President, Legal, Privacy and Regulatory
CLEAR

Despite a growing and evolving legitimate user base, cryptocurrency—like cash—remains a popular means by which a wide range of criminal activities are funded and the proceeds of such activities are distributed. Cryptocurrency's decentralized, pseudo-anonymous nature, and the ease with which it can be moved across national borders with limited government oversight, make it attractive to cybercriminals, narcotics traffickers, and international organized crime groups, to name a few.

This article is meant to complement the recently published Department of Justice (Department) *Cryptocurrency Enforcement Framework* and build on the highly useful article that appeared in the 2019 Cybercrime and Cyber Threats edition of this journal: *Attribution in Cryptocurrency Cases*.[1] In the past two years, we have seen continued proliferation in the use of cryptocurrency by criminals and, far more concerningly, significant evolution in the means by which criminals can foil law enforcement authorities' efforts to develop attribution based on blockchain analysis. At the same time, however, the blockchain analysis tools available to law enforcement—many provided by third-party vendors—have become increasingly powerful and effective. This article seeks to survey the state of blockchain analysis in federal criminal investigations and to explore approaches for leveraging that analysis, both in the initial stages of an investigation and, far more interestingly, at trial.

---

[1] Michele R. Korver, et al., *Attribution in Cryptocurrency Cases*, 67 DOJ J. FED. L. & PRAC., no. 1, 2019, at 233.

The first section of this article provides the technical framework for how cryptocurrency works, how blockchains may be analyzed, and ways those analysis techniques can be foiled or otherwise complicated. The second section describes how blockchain analysis can be used at the start of an investigation or in search warrant affidavits and other criminal process to advance such an investigation. The third and final section discusses ways to admit blockchain evidence at trial, as well as important considerations when admitting such evidence, including approaches to satisfying discovery obligations.

I. Introduction and background

A. What is a blockchain?

First, some necessary vocabulary and background: `Cryptocurrency`, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange.[2] Cryptocurrency users have one or more `addresses`, somewhat similar to bank account numbers and consisting of long strings of numbers and letters that users can trivially generate. Those addresses, on their own, have no correlation to their owners' real-world identities. Each address is a representation of a `public key` and has a corresponding `private key` that controls the ability to spend funds associated with the address.[3]

Cryptocurrencies are generally based on a distributed transaction ledger system called a `blockchain`.[4] A blockchain comprises a series of blocks, each of which contains data regarding batches of valid transactions. Each block also contains a cryptographic hash of the prior block of the blockchain, linking the blocks together and forming a chain of transactional information going back to the beginning of the ledger.

With a Bitcoin transaction from *A* to *B*, for example, the blockchain entry for that transaction will include three particularly significant categories of information:

---

[2] *Id.* at 233.

[3] For a more detailed discussion of cryptocurrency fundamentals, see JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS (2015).

[4] For a more detailed discussion of blockchains and how blockchains serve as cryptocurrency transaction records, see Peter Van Valkenburg, *What's a Blockchain, Anyway?*, COIN CTR. (Apr. 25, 2017), https://www.coincenter.org/education/blockchain-101/whats-a-blockchain/.

- one or more `inputs`—that is, the source (or sources) of the bitcoin being transferred in the transaction from *A* to *B*;
- an `amount`—that is, how much *A* transfered to *B*; and
- one or more `outputs`—that is, *B*'s Bitcoin address, or where the bitcoin should be transferred.

To initiate such a transaction using funds from her address, *A* (the payer) must cryptographically sign the transaction with her address' private key, which was generated when that address was created. Only the holder of a private key for a Bitcoin address can spend bitcoin from the address. A Bitcoin user can also spend from multiple Bitcoin addresses in a single transaction.

When a user creates a new transaction, she broadcasts that transaction to all the nodes in the network. Certain members of the network (often called `miners`) validate the transaction and include it in a proposed block. Eventually, the block containing that transaction (along with others) is added to the chain. On the Bitcoin blockchain, a new block is created every ten minutes, on average, and with each block, an average of approximately 2,000 new transactions are added to the blockchain.[5] The blockchain is constantly updated and stored by full nodes—members of the Bitcoin network, including many miners, who store and share full copies of the blockchain.

The transactional information contained in the blockchain does not explicitly identify the parties to any given transaction. By analyzing the blockchain, however, it is possible, in some cases, to identify (or make a reasonable inference about) the owner of a particular Bitcoin address.

B. Blockchain analysis techniques

Because details of every transaction are stored within the blockchain, the most conceptually intuitive type of blockchain analysis involves reviewing the transaction history and following the movement of funds over time from one address to another—a process

[5] For a more detailed discussion on mining, see Peter Van Valkenburg, *What is Bitcoin Mining, and Why is it Necessary?*, COIN CTR. (Dec. 5, 2014), https://www.coincenter.org/education/advanced-topics/mining/.

sometimes called tracing.[6] With Bitcoin, for example, anyone can see any Bitcoin transaction since the inception of that cryptocurrency, either by downloading a copy of the blockchain through the network itself or by using a publicly available blockchain explorer, such as the one available at blockchain.com/explorer. Attempted manually, such tracing is cumbersome and time consuming, but a growing collection of new technology companies offer tools to make this analysis faster and more efficient.

Of course, tracing the movement of funds along the blockchain does not necessarily identify a specific address owner or party to a particular transaction. But the owners of some addresses can be identified through a number of ways off-chain—that is, based on information obtained from a source other than the blockchain itself. For example, users sometimes post their Bitcoin wallets on social media and forums. Labeling an address with a real-world identity is sometimes called tagging. And where tracing analysis leads through one or more tagged addresses, making highly probable inferences about a transaction's participants becomes increasingly possible.

Another blockchain analysis technique is identifying linked addresses (or clusters) held by an individual or organization. One common protocol for cluster analysis is linking together all the input addresses for one transaction. That is, if two or more addresses are inputs of the same transaction with one output, then one can infer that those input addresses are controlled by the same user. This common input or co-spend analysis is highly reliable and is the most-used metric in commercial blockchain analysis tools. Another clustering heuristic is to identify a transaction's change address, which is the sender's address that receives any remainders of transferred funds from a transaction that spends a smaller amount of virtual currency than the amount associated with the sender's input(s). If such a change address is identified, then the ultimate output of that address and all the original inputs of the transaction may be controlled by the same user. While clustering can be done manually, doing so would be cumbersome and limited; instead, law

[6] This is true for Bitcoin and other cryptocurrencies with public blockchains. Other "anonymity enhanced cryptocurrencies" use non-public blockchains, making it much more difficult to trace funds.

enforcement uses commercially available blockchain analysis tools to streamline the process.[7]

Law enforcement and regulators use a wide range of blockchain analysis tools to apply these analysis techniques, many of which are provided by third-party companies like Chainalysis, TRM Labs, and Elliptic. There are also free basic blockchain analysis tools that allow users to view the transaction history associated with a given address. While those free tools may allow the user to perform some basic tracing, they, unfortunately, are often incapable of employing clustering or other more involved techniques for tracing or attributing more complex cryptocurrency transaction histories.

C. Obfuscating the transaction history on the blockchain

Clustering, off-chain data scraping, tracing, and other blockchain analysis techniques can be foiled by a variety of cryptocurrency money laundering techniques popular with even relatively unsophisticated criminals. For example, third-party crypto `mixing`—or `tumbling`—services shuffle a user's bitcoins with other users' cryptocurrency to release a fresh batch of bitcoins from a random address. The process, which users typically pay a variable fee for, breaks the transaction trail and usually makes tracing highly impractical.

Another obfuscation technique is known as `chain hopping`, moving assets from one cryptocurrency to another, often through a rapid succession of transactions. Paid chain-hopping services specialize in executing these transfers in a manner that may make them very difficult for investigators to detect and analyze. This difficulty is exacerbated when the chain hopping involves anonymity enhanced cryptocurrencies with non-public blockchains.

`Peel chains` are another means by which users obfuscate blockchain transaction histories. A peel chain occurs when a large amount of bitcoin sitting at one address is sent through a series of transactions in which a slightly smaller amount of bitcoin is transferred to a new address with each transaction. In each of these steps, some quantity of bitcoin "peels off" the chain to another

---

[7] *See, e.g.,* United States v. Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020) (stating that no Fourth Amendment privacy interest existed where agents used an outside service to analyze the publicly viewable Bitcoin blockchain and identify a cluster of Bitcoin addresses controlled by the targets).

address—frequently to be deposited into a virtual currency exchange—and the remaining balance is transferred to the next address in the chain. This technique is growing in popularity: Peel chains were employed by North Korea-based cybercriminals targeted in a recent case out of the District of Columbia.[8]

II. Blockchain analysis in investigations

Many criminal cases begin and end successfully when investigators remember the wise adage, "follow the money." This strategy holds with cryptocurrency, and investigators increasingly rely on blockchain analysis to both identify criminal actors and build a case against them. As you consider whether and how to incorporate blockchain analysis into your investigative strategy, be forewarned: There may be myriad challenges—legal and practical—to admitting blockchain analysis evidence at trial. For example, some analytical tools may incorporate sensitive or proprietary techniques that cannot be readily presented in open court. As discussed further below, these difficulties are hardly insurmountable, but a savvy prosecutor may conclude that employing tools in other ways that avoid undue litigation risk may be the more prudent course.

Given these challenges, consider from the outset what role blockchain analysis should play the investigation. Of course, the answer may be dictated by simple necessity, such as where there is no other viable avenue for developing attribution evidence.

A. Tips and leads for identifying investigative targets

Many successful investigations begin with a tip from a confidential source. The admissibility—even the veracity—of such "tips and leads" are rarely, if ever, the subject of litigation.[9] Likewise, blockchain analysis can be a useful tool simply for identifying investigatory targets of merit.

---

[8] Complaint, United States v. 113 Virtual Currency Accounts, No. 20-cv-606 (D.D.C. Mar. 3, 2020), ECF No. 1.

[9] A grand jury needs no probable cause to initiate an investigation. The impetus for the investigation may be "tips, rumors, evidence proffered by the prosecutor, or the personal knowledge of the grand jurors." Branzburg v. Hayes, 408 U.S. 665, 701 (1972).

Investigators can identify addresses of interest through online undercover operations or publicly posted addresses on criminal forums, or through a transaction analysis to flag large payments or especially active addresses. And once a subject address is identified, a tracing analysis can provide investigators with a sense of scope—that is, how much money has moved into and out of a particular wallet associated with a darknet child pornography marketplace or known jihadist forum over a longer period of time?

In addition to these techniques for proactively identifying addresses that may be engaged in illicit activities, investigators may also receive valuable leads from cryptocurrency exchanges, which are considered money services businesses (MSBs) and, thus, are obligated to have anti-money laundering programs and file suspicious activity reports (SARs) and other notifications under the Bank Secrecy Act. Subpoenas to cryptocurrency exchanges may even allow investigators to obtain valuable attribution evidence as to the owner of a particular address.[10]

Once a target is identified based on suspicious cryptocurrency transactions, a SAR from an exchange, or other such methods, investigators may conclude that further blockchain analysis is not necessary or worthwhile, electing instead to pursue more traditional investigative techniques—ranging from real-world surveillance to social media search warrants—to build a case against the individual. By treating suspicious cryptocurrency transactions and any associated blockchain analysis as tips and leads only, investigators will forego the use of evidence from blockchain analysis in their case-in-chief, but they will also avoid the evidentiary and logistical challenges associated with using of such evidence at trial.

B. Use in criminal process

In addition to using blockchain analysis for pure lead purposes, it can also be used in search and seizure warrants. Similar to instances where blockchain analysis leads to a subpoena or a Financial Crimes Enforcement Network database query at the initiation of an investigation, its use in warrants is often an intermediate step used to justify searching a subject's residence, digital devices, or other

[10] This is true with centralized exchanges that are responsive to legal process. Peer-to-peer transactions conducted via decentralized exchanges (DEXs) may foil such efforts at attribution, however.

location—with the understanding that the fruits of that search (such as drug paraphernalia, child pornography, incriminating text messages, etc.) will provide the primary evidence of the subject's guilt at trial, rather than the blockchain analysis.

That raises the question of how courts should weigh blockchain analysis in evaluating probable cause for a search or seizure. As the Supreme Court has stated, probable cause requires only a "'fair probability' on which 'reasonable and prudent [people,] not legal technicians, act.'"[11] "[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules."[12] Under this "totality-of-the-circumstances approach," there is no one-size-fits-all approach to using blockchain analysis in warrant applications.[13]

1. Lessons from the law of anonymous tips

A starting point for analysis might be how courts assess information from informants or anonymous tipsters. One representative formulation by the Seventh Circuit holds that probable cause depends on the informant's "reliability, veracity and basis of knowledge."[14] Of these factors, reliability is probably the most important to address for blockchain analysis. Few questions should arise about the basis of knowledge or veracity. The basis of knowledge for blockchain analysis—that is, the source of information used to conduct such analysis—is, generally speaking, the blockchain itself.[15] The blockchain is an open-source, publicly available database relied upon by users around the world for up to hundreds of thousands of

---

[11] Florida v. Harris, 568 U.S. 237, 244 (2013) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)) (alteration in original).
[12] *Gates*, 462 U.S. at 232.
[13] *Id.* at 230.
[14] United States v. Orr, 969 F.3d 732, 736 (7th Cir. 2020) (quoting United States v. Olson, 408 F.3d 366, 370 (7th Cir. 2005)); *see also Gates*, 462 U.S. at 230 (stating that veracity, reliability, and basis of knowledge "should be understood simply as closely intertwined issues that may usefully illuminate the common-sense, practical question whether there is 'probable cause' to believe that contraband or evidence is located in a particular place").
[15] More sophisticated applications of blockchain analysis may draw on other sources of information for attribution or more accurate clustering.

transactions per day.[16] There is no serious question that the blockchain accurately captures the transactional data used in blockchain analysis. In a similar vein, the blockchain is the product of an automated process (for example, the Bitcoin protocol), so it makes little sense for a court to question the veracity of the data the way it might inquire into the motives or trustworthiness of an informant.

Reliability is a more complicated question: Can you reliably use blockchain analysis to trace funds from one wallet address to another? At its most basic level, blockchain analysis is not that much different than tracing funds from one bank account to another. If attribution is not at issue—for example, in a seizure warrant intended to recover the proceeds of a fraud or hack—it may be enough for the warrant to list out the "audit trail" of hops from the originating address to the final resting point. In a sense, this is not really blockchain "analysis" at all; it is simply using the blockchain as a source of transactional information, just as an affidavit might rely on bank records to show the transfer of funds from a victim's bank account, through intermediary accounts, to the account targeted for seizure.

In other cases, blockchain analysis might be used to explain audit trails that are too long or too complicated to be narrated in detail, or to show attribution and ownership through a series of transactions (such as a peel chain). Here, it may be appropriate for the affidavit to address the reliability of blockchain analysis as used to support probable cause. There are several possible approaches.

First, the affidavit could identify the underlying assumptions and logic used in grouping clusters—such as co-spending or change addresses—and explain that the assumptions are based on commonly observed patterns of transactional behavior. Second, the affidavit could note the generally reliable track record of blockchain analysis in other contexts.[17] This might include similar investigations conducted by law enforcement. It might also include the growing use of blockchain analysis in the private sector as a due diligence and anti-money laundering (AML) tool. Third, the affidavit could cite other

---

[16] *See Bitcoin*, COINDESK, https://www.coindesk.com/price/bitcoin (last visited Feb. 11, 2021) (showing 340,736 transactions valued at $12.45 billion during preceding 24-hour period).

[17] *See* United States v. Bradley, 924 F.3d 476, 480 (8th Cir. 2019) ("An 'informant's track record of providing trustworthy information' establishes reliability.") (quoting United States v. Faulkner, 826 F.3d 1139, 1144 (8th Cir. 2016)).

corroborating evidence generated in the investigation.[18] For example, in a drug trafficking investigation, blockchain analysis might be used to identify a subject cashing out cryptocurrency proceeds derived from a darknet vendor—perhaps through a long, complicated chain of transactions that eventually winds up at an identifiable exchange account. Here, blockchain analysis serves two functions: It traces the transactions, and it attributes them to a single actor engaged in multiple laundering transactions (as opposed to multiple independent actors engaged in one-off commercial transactions). Thus, to the extent there is other, more traditional evidence linking the subject to drug trafficking activity, that evidence serves to corroborate the critical attribution element of the blockchain analysis.

2. Comparison to software used in child pornography investigations

To our knowledge, there are no published decisions analyzing the weight or reliability of blockchain evidence in a search warrant application.[19] But—with important caveats—some lessons might be

---

[18] *See* United States v Colkley, 899 F.2d 297, 302 (4th Cir. 1990) (reasoning that an anonymous tip "was sufficiently detailed and sufficiently corroborated by independent police work to come within the standards of probable cause articulated in *Gates*").

[19] On January 6, 2021, a magistrate judge in the District of Columbia issued a Rule 41 premises search warrant for the home of a subject suspected of using bitcoin to purchase child pornography from an Tor-based child pornography website, authorizing, *inter alia*, the seizure of cryptocurrency found at the premises used to commit and promote the child pornography offenses. *See In re* Search of One Address in Washington, D.C. Under Rule 41, No. 20-sw-314, 2021 WL 49928 (D.D.C. Jan. 6, 2021) [hereinafter *Search of One Address*]. In a written opinion accompanying the warrant, the court noted that blockchain analysis was responsible for identifying the cryptocurrency exchange used by the illegal website, and that records from the cryptocurrency exchange in turn revealed the identity of the subject. *Id.* at *2 ("Blockchain analysis revealed that Website 1 used a 'payment processing service . . . operated by a known cryptocurrency exchange service (the "Exchange") located in the United States' to effectuate the illicit transactions. By subpoenaing the Exchange, law enforcement obtained documents revealing the identity of the Subject.") (quoting warrant affidavit) (internal citations omitted). The court did not, however, expound on how much weight it placed on the blockchain analysis in the overall determination of probable cause to search the subject premises.

drawn from the growing body of case law affirming the use of automated software tools in child pornography investigations to identify users sharing child exploitation material online. For example, in *United States v. Thomas*, the Second Circuit considered a warrant based primarily on a proprietary software suite known as Child Protection System (CPS).[20] As the Second Circuit explained, CPS simply automates the process of a law enforcement officer manually querying peer-to-peer (P2P) file sharing networks for known child exploitation material: "CPS automates this process by canvassing these public P2P networks, identifying files that contain child pornography, cataloguing this information, and providing law enforcement officers with a list of the online users who are sharing these files over P2P networks."[21] In *Thomas*, CPS was used to identify a suspect Internet Protocol (IP) address, which agents then used to identify a physical address, conduct surveillance, and obtain a search warrant. The Second Circuit held that the CPS software established sufficient probable cause to link the illicit activity to the target premises, emphasizing the fact that the software merely automated a process that could otherwise be done manually.[22] That was sufficient to distinguish the use of CPS software from drug-sniffing dogs, the proper employment of which requires "numerous steps, each of which is susceptible to error."[23] The Sixth Circuit followed suit in *United States v. Dunning*, relying in part on *Thomas* to affirm the sufficiency of an affidavit based on CPS.[24] In addition, the Sixth Circuit cited the affiant's training and experience with the software, noting that he "was trained to use, and had previously used, software to investigate child pornography crimes."[25]

Like the software tools described above, blockchain analysis software largely serves an aggregation function. In theory, most analysis of blockchain transactions could be done by hand. But in cases involving hundreds, or perhaps thousands, of transactions—given the ability of criminals to generate limitless new addresses and to use software tools to create automated spending algorithms—much of the functionality provided by blockchain analysis software lies in its

[20] 788 F.3d 345, 348 (2d Cir. 2015).
[21] *Id.*
[22] *See id.* at 352.
[23] *Id.*
[24] 857 F.3d 342, 347–48 (6th Cir. 2017).
[25] *Id.* at 347.

ability to pull massive amounts of transactional data from the blockchain and provide user-friendly tools to explore it.[26] To be sure, there are limits to this analogy. Blockchain analysis software does not *only* aggregate blockchain data; it also applies heuristics and other analytical tools to cluster addresses into related groups. But not every warrant needs to rely on those additional functions. To the extent blockchain analysis software is used simply to "follow the money" in a warrant affidavit, cases like *Thomas* and *Dunning* should lend support.

This line of cases has yielded a few additional points that are relevant to using proprietary blockchain analysis software platforms to support probable cause in an affidavit. First, neither the identity of the specific company nor the underlying software code is important to the probable cause analysis. As the Second Circuit explained in *Thomas*, "the primary relevance of automating third-party software lies not in its name, but in its *functionality*," and it was sufficient where "the affidavit disclosed that law enforcement used automated software during the course of this investigation, noted the software's purpose, and then went into considerable detail as to how the software operated."[27] Second, the software's conclusions need not rise to the level of scientific certainty to establish probable cause.[28] And third, courts have carefully distinguished between the use of software tools to establish probable cause in a warrant from their admissibility at

---

[26] *See, e.g.*, *Search of One Address*, 2021 WL 49928, at *2 (noting that "law enforcement can use publicly-available software to analyze the BTC blockchain by 'forensically examining, tracing, and mapping data on the blockchain . . . to unmask the identities of specific users of a given cryptocurrency wallet'") (quoting search warrant affidavit).

[27] *Thomas*, 788 F.3d at 351; *cf. Dunning*, 857 F.3d at 346–47 (rejecting defense argument that affidavit could not rely on CPS without explaining software's "source code").

[28] *See, e.g.*, United States v. Chiaradio, 684 F.3d 265, 279 (1st Cir. 2012) (rejecting defense challenge to scientific reliability of EP2P software "[b]ecause probable cause 'does not require scientific certainty'") (quoting Roche v. John Hancock Mut. Life Ins. Co., 81 F.3d 249, 254 (1st Cir. 1996)); United States v. Schumacher, 611 F. App'x 337, 340 (6th Cir. 2015) (not precedential) (rejecting defense challenge based on "scientific reliability" of software).

trial.[29] This is a particularly important point for blockchain analysis: Probable cause and admissibility are different questions, governed by different standards and separate bodies of law. Prosecutors should resist efforts by courts or defense counsel to view warrant applications through the lens of technical evidentiary rules.

C. Blockchain analysis in civil forfeiture complaints

Finally, two recent civil forfeiture actions involving cryptocurrency thefts linked to North Korea provide public examples of blockchain analysis in action.[30] It should be noted that civil forfeiture complaints are not the same as warrant affidavits. They are subject to a lower standard of proof than search warrants.[31] At the same time, they are public pleadings used to announce the government's case—roughly equivalent to an indictment or criminal complaint—and may include more detail than strictly necessary to meet the relevant legal threshold. In any event, these complaints offer rare public examples, readily adaptable to warrant affidavits, of how blockchain evidence can be described and relied upon.

The complaints include a succinct introduction to blockchain analysis in their background sections. For example:

> While the identity of a BTC/ETH address owner is generally anonymous (unless the owner opts to make the information publicly available), law enforcement can identify the owner of a particular BTC/ETH address by analyzing the blockchain. The analysis can also reveal additional addresses controlled by the same individual or entity. For example, a user or business may create many BTC addresses to receive payments from different customers. When the user wants to transact the BTC that it has received (for example, to exchange BTC for

---

[29] *See, e.g.*, *Chiaradio*, 684 F.3d at 279 (rejecting defense argument that software was "too untested to meet the requirements of the Federal Rules of Evidence" because "[t]his argument mixes plums and pomegranates; the Federal Rules of Evidence do not apply" to the probable cause standard).
[30] Complaint, *supra* note 8; Complaint, United States v. 280 Virtual Currency Accts., No. 20-CV-02396 (D.D.C. Aug. 27, 2020), ECF No. 1 [hereinafter Complaint, *280 Virtual Currency Accts.*].
[31] *See* United States v. Mondragon, 313 F.3d 862, 864–66 (4th Cir. 2002) (reasonable belief).

> other currency or to purchase goods or services), it may group those addresses together to send a single transaction. Law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze the blockchain and attempt to identify the individuals or groups involved in the virtual currency transactions. Specifically, these companies create large databases that group transactions into "clusters" through analysis of data underlying the virtual currency transactions.[32]

A similar summary of blockchain analysis could be included in warrant affidavits, especially in cases where blockchain analysis is used in more sophisticated ways to cluster and attribute addresses.[33]

The complaints also cite or refer to blockchain analysis when discussing specific transactions. For example, in discussing a publicly reported hack of a cryptocurrency exchange, the complaint in *280 Virtual Currency Accounts* explains that "[b]lockchain analysis corroborated [the exchange's] statements and provided more detail for the following thefts/transactions."[34] In another example, blockchain analysis was used to trace funds through a series of clusters; the complaint explains that the pattern "illustrat[es] common ownership as the funds regroup at the same destination after being layered."[35] Nevertheless, not every element of the narrative relies on the analytical functions of blockchain analysis—at multiple points, the complaints simply list out individual transactions or include charts showing the step-by-step movement of funds. The same approach could be taken in a warrant affidavit.

III. Blockchain analysis at trial

In recent years, virtual currency use has dramatically expanded, as has criminal investigation and prosecution of crimes involving virtual

---

[32] Complaint, *280 Virtual Currency Accts.*, *supra* note 30, at ¶ 13.
[33] A concise overview of blockchain tracing methodology also appears in *Search of One Address*, 2021 WL 49928, at *2.
[34] Complaint, *280 Virtual Currency Accts.*, *supra* note 30, at ¶ 27.
[35] *Id.* ¶ 44.

currency.[36] Despite the broad use of blockchain analysis in a variety of cases, see Section II., *supra*, litigation regarding its admissibility has been limited.[37] Some legal writers—albeit mostly law students—have even questioned its admissibility entirely.[38] Luckily, examining the Federal Rules of Evidence reveals multiple clear paths to the admission of blockchain evidence.[39] This section discusses methods for authenticating blockchain evidence, clarifies why the blockchain should not be excluded as hearsay and does not present a Confrontation Clause problem, and addresses trial strategies for

---

[36] *See generally* U.S. DEP'T OF JUST., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASKFORCE: CRYPTOCURRENCY ENFORCEMENT FRAMEWORK (Oct. 2020).

[37] The earliest instance of blockchain evidence being admitted in a significant federal trial appears to be the Silk Road trial in 2015. There, the government used screenshots from Blockchain.info to depict the Bitcoin transactions related to the Silk Road Marketplace. Transcript at 1729–32., United States v. Ulbricht, 14-cr-68 (S.D.N.Y Jan. 29, 2015), ECF No. 212. This approach was similarly taken by the government in *United States v. Michael Brown* the following year. Transcript, *United States v. Brown,* No. 3:13-cr-118 1, 98 (M.D. Tenn. May 10, 2016) (Where the Blockchain.info records were particularly relevant because the defendant visited the Blockchain.info page for the bitcoin address at issue). Bitcoin and/or blockchain-related evidence has also been admitted in, *inter alia*, *United States v. Costanzo,* 956 F.3d 1088 (9th Cir. 2020) and *United States v. Ologeanu*, No. 18-cr-81, 2020 WL 1676802, at *10–*11 (E.D. Ky. Apr. 4, 2020).

[38] *See, e.g.*, Angela Guo, *Blockchain Receipts: Patentability and Admissibility in Court*, 16 CHI.-KENT J. INTELL. PROP. 440, 444–45 (Apr. 2017) ("[T]he admissibility of these distributed ledger receipts has not been entirely settled."), J. Collin Spring, *The Blockchain Paradox: Almost Always Reliable, Almost Never Admissible*, 72 SMU L. REV. 925, 935 (2019) ("blockchain evidence is almost always inadmissible in federal court, and is only admissible under limited, factually specific scenarios."). *But see* George Bellas, *Blockchain as Evidence*, 66 ILL. STATE BAR ASS'N–TRIAL BRIEFS NO. 3 (Nov. 2019) (observing that introducing blockchain data as evidence at trial "[s]ounds daunting, but it is really not that complicated," while discussing the applicability of Illinois state rules of evidence that parallel the federal rules).

[39] To avoid any issue, Vermont went so far as to enact legislation specifically declaring blockchain evidence self-authenticating. H.868 (Act 157) (Vt. 2016) ("A digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence 902.").

admitting blockchain evidence and related testimony before concluding with a brief discussion of discovery considerations.

A. Authentication

As explained in Section I., *supra*, a blockchain is an immutable ledger that serves as a tamper-proof record of all confirmed transactions.[40] The blockchain serves as the ground truth for cryptocurrency transactions—if a transaction is recorded on a blockchain, the transaction definitively occurred, because its presence on the blockchain is what defines the transaction's occurrence.[41] Metaphysics aside, the blockchain is inherently well-positioned to address the core goal of the authentication requirements of the Federal Rules of Evidence—to show that proffered evidence is what the proponent claims it to be.[42]

Rule 901 sets forth a non-exhaustive list of common methods for authenticating evidence. The applicability of several of the methods to blockchain evidence is addressed below. Prosecutors should be mindful that the methods enumerated in Rule 901 are illustrative, not comprehensive. Indeed, when considering authentication of electronic evidence, at least some courts "have been willing to think 'outside of the box' to recognize new ways of authentication."[43]

1. Witness with knowledge

One of the easiest ways to authenticate the blockchain is perhaps the most easily overlooked—through the testimony of a foundation witness.[44] For most virtual currencies, the blockchain is publicly available and can be downloaded directly by any member of the network.[45] The Bitcoin blockchain file is over 300 GB and growing

---

[40] *See Gratkowski*, 964 F.3d at 309 n.2 (defining blockchain as "a technological advancement that permits members in a shared network to 'record a history of transactions on an immutable ledger.'").

[41] *See Costanzo*, 956 F.3d at 1093 ("Each transaction was complete only after it was verified on the blockchain.").

[42] FED. R. EVID. 901.

[43] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 552 (D. Md. 2007).

[44] FED. R. EVID. 901(b)(1).

[45] For the purposes of this article, we have focused on publicly available blockchains. Presenting evidence regarding transactions conducted through anonymity-enhanced cryptocurrencies (AECs) may necessitate different considerations.

constantly with each new block that is confirmed.[46] A government witness versed in virtual currency could easily download a copy of the blockchain and explain it conceptually to the jury. Such testimony would also readily fit within Rule 901(b)(9), evidence about a process or system,[47] and could be bolstered by a discussion of the distinctive characteristics of the blockchain pursuant to Rule 901(b)(4),[48] all of which would aid in authenticating the evidence.

2. Rule 902 certifications

While prosecutors offering blockchain evidence will almost certainly want to offer testimony to put it into context, see Section III.C., *infra*, there are several options for admitting blockchain evidence as self-authenticating under Rule 902. This may help avoid the unnecessary hassle of calling a witness purely for authentication purposes.[49]

In many cases, blockchain records may be admitted as business records under Rule 902(11).[50] This rule allows a record that meets the requirements of Rule 803(6) to be admitted with a certification from the records custodian.[51] Rule 803(6), discussed further in Section III.B., *infra*, pertains to a record of, *inter alia,* an act, event, or condition where the record was "made at or near the time by—or from information transmitted by—someone with knowledge" and "kept in the course of a regularly conducted activity of a business, organization, occupation, or calling," where "making the record was a

---

[46] *Blockchain Size (MB)*, BLOCKCHAIN.COM, https://www.blockchain.com/charts/blocks-size (last visited Feb. 11, 2021.).

[47] FED. R. EVID. 901(b)(9).

[48] FED R. EVID. 901(b)(4).

[49] *Contra* Michael L. Levy & John M. Haried, *Practical Considerations When Using New Evidence Rule 902(13) to Self-Authenticate Electronically Generated Evidence in Criminal Cases*, 67 DOJ J. FED. L. & PRAC. no. 1, 2019, at 84 ("With unfamiliar technology, it is certainly conceivable that some judges will not be satisfied with anything less than a live witness explaining the process.").

[50] Guo, *supra* note 38, at 448. ("The blockchain receipts and the consensus algorithm are quintessential examples of record-keeping in the ordinary course of business.").

[51] FED R. EVID. 902(11).

regular practice of the activity."[52] Courts have confirmed that "computer data compilations" may be business records.[53]

The blockchain is a living record, with new blocks of transactions being appended with each confirmation at roughly 10-minute intervals. This easily satisfies the temporal element of the first requirement, that the record be made at or near the time of the transaction. The record is made by the miner validating the transaction block, based on the information relayed to it by the computers announcing the proposed transactions. (Alternatively, if a court determines that the virtual currency transactions are hearsay-eligible statements of the sender rather than computer-generated records, the "someone with knowledge" would be the sender himself, who transmitted the information to the other members of the virtual currency network upon signing and announcing the transaction.) The blockchain is necessarily kept in the course of miners' and node operators' regularly conducted activity, and making the record is a regular practice of their activity—indeed, the maintenance of the blockchain is the core function of these virtual currency participants. It bears emphasizing that this analysis is not limited to miners but applies to many parties that operate nodes and keep and maintain a copy of the blockchain as part of their regularly conducted activity.

Prosecutors may have multiple options in determining who should certify the blockchain records. Rule 902(11) allows the certification to be completed by "the custodian or *another qualified person*."[54] As the advisory committee notes to Rule 803(6) comment, there is no requirement that the witness be involved as a participant in the matters reported.[55] Rather, the records may be admitted through someone acting merely as an observer.[56] Indeed, courts have long held that the other "qualified witness" only need to understand the record

---

[52] FED R. EVID. 803(6).
[53] Rosenberg v. Collins, 624 F.2d 659, 665 (5th Cir. 1980); United States v. Fendley, 522 F.2d 181 (5th Cir. 1975).
[54] FED. R. EVID. 902(11) (emphasis added).
[55] FED. R. EVID. 803(6) advisory committee's note to 1972 proposed rules ("Occasional decisions have reached for enhanced accuracy by requiring involvement as a participant in matters reported. . . . The rule includes no requirement of this nature. Wholly acceptable records may involve matters merely observed . . .").
[56] *Id.*

keeping system to authenticate the evidence.[57] This is significant in the blockchain context: It confirms that one need not be a miner or the operator of a full node involved in relaying and verifying transactions to appropriately certify the blockchain. Rather, any individual who directly obtains a copy of the blockchain and meets the remaining requirements under 803(6) may provide a certification under 902(11). This may extend to virtual currency exchanges, wallet hosting providers, law enforcement blockchain specialists, academics, and even blockchain enthusiasts. An analyst specializing in blockchain analysis who regularly maintains a copy of the blockchain to perform her blockchain analysis duties in her organization would easily meet the requirements for providing a certification under 902(11).

Blockchain evidence may also be authenticated using a certification issued pursuant to Rule 902(13). Under Rule 902(13), certified records generated by an electronic process or system that produces accurate results are self-authenticating.[58] Rule 902(13) was adopted in December 2017 and sought to make it easier for parties to authenticate certain types of electronic evidence without "the expense and inconvenience of producing a witness" unnecessarily.[59]

The core code underlying Bitcoin and most decentralized virtual currencies[60] is designed to ensure that the blockchain is resistant to any attempted manipulation. The entire transaction verification and validation process is intended to further bolster the sanctity of the

---

[57] United States v. Salgado, 250 F.3d 438, 452–53 (6th Cir. 2001) (the authenticating witness must merely be "familiar with the record keeping system employed" but need not have programmed the computer herself or be an expert on the details of the computer processes pursuant to which the records are created, maintained, and produced). Levy & Haried, *supra* note 49, at 86 (citing United States v. Ray, 930 F.2d 1368, 1369–70 (9th Cir. 1990); United States v. Franco, 874 F.2d 1136, 1139–40 (7th Cir. 1989); United States v. Hathaway, 798 F.2d 902, 905–07 (6th Cir. 1986)).

[58] FED. R. EVID. 902(13).

[59] FED. R. EVID. 902(13) advisory committee's note to 2007 amendment.

[60] Prosecutors dealing with non-mainstream virtual currencies with smaller user bases that may have adapted their code in a way that introduced security vulnerabilities or allow for transaction manipulation (inadvertently or intentionally) will need to provide additional facts to show that the blockchain records for that particular virtual currency were the product of a process or system that produces an accurate result. Even given the thousands of virtual currencies currently in existence, this is likely to be a real consideration in only a very small number of cases.

data contained in the blockchain. As explained in Section I., *supra*, virtual currency transactions are signed by the sender's private key, validated by nodes, confirmed by miners, and then added to the blockchain, whereupon subsequent node operators and miners affirm the integrity of the transaction by accepting the block in which the transaction is contained and adding new blocks on top of it. In short, the blockchain has extensive built-in protections to ensure the system or process produces an accurate result.

The addition of Rule 902(13), along with Rule 902(14)—which deals with authenticating forensic images and was adopted at the same time—was accompanied by several noteworthy pieces of legal scholarship discussing the applicability of the rules.[61] Much of the discussion incorporated scenarios developed by John Haried, Criminal eDiscovery Coordinator at the Department, who originally proposed the amendments at the advisory committee's symposium on electronic evidence.[62] In collaboration with the reporter to the Evidence Rules Committee, Haried developed several hypotheticals articulating the applicability of the new rules to particular fact patterns. These scenarios and the related analysis were incorporated into a treatise on authenticating digital evidence co-authored by the reporter to the Judicial Conference Advisory Committee on Evidence Rules and former members of Judicial Conference advisory committees, including the Honorable Paul Grimm, widely regarded as an expert in electronic evidence matters.[63] In general, the applicability of the rules to the stated scenarios carries far more persuasive and authoritative weight than would otherwise be warranted for analysis contained in a typical law review article.

A review of these scenarios provides useful corollaries to admitting blockchain evidence. In one, the proponent uses Rule 902(13) to authenticate a web server log that automatically records certain information about every computer that views a website and captured the hacker-defendant's IP address.[64] In another, the proponent uses

---

[61] John M. Haried, *Two New Self-Authentication Rules That Make It Easier to Admit Electronic Evidence*, 66 U.S. ATTY'S BULL., no. 1, 2018, at 127; Paul W. Grimm et al., *Authenticating Digital Evidence*, 69 BAYLOR L. REV. *1 (2017); Levy & Haried, *supra* note 49, at 81.

[62] *See* Grimm, *supra* note 61, at *42 n.138; Symposium, *The Challenges of Electronic Evidence*, 83 FORDHAM L. REV. 1163, 1192–97 (2014).

[63] Grimm, *supra* note 61, at *42 n.138.

[64] *Id*. at *43–*44.

Rule 902(13) to authenticate records from the Windows registry indicating that a particular USB drive was plugged into a particular computer:

> With Rule 902(13), the proponent of the evidence could obtain a written certification from the forensic technician, stating that the Windows operating system regularly records information in the Windows registry about USB devices connected to a computer; that the process by which such information is recorded produces an accurate result; and that the printout accurately reflected information stored in the Windows registry of [the defendant's] computer.[65]

The blockchain is much like the web server log or Windows registry log discussed in the hypotheticals above, except it records and stores records of virtual currency transactions, rather than records of IP address access to a server or USB drive connections to a computer. The blockchain also produces an accurate result, recording the virtual currency transactions in their true form. The additional verification and validation protections built into the blockchain ensure a result even more accurate than that contemplated by a web server log or Windows registry log.[66]

To satisfy Rule 902(13), the certification may need to provide additional background regarding the blockchain to establish the reliability of the system or process.[67] As the advisory committee notes explain, the certification must provide information that would be sufficient to authenticate the record if the certifying person testified.[68]

---

[65] *Id.*

[66] *See generally* United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988) (Once authenticated, questions about the accuracy of computer-generated records resulting from incorrect data entry or the operation of the computer program affect "only the weight of the printouts, not their admissibility.").

[67] *See generally* Levy & Haried, *supra* note 49 (Observing that "[m]achine-generated records from less familiar systems and processes . . . may require a more factually detailed certification," and noting that a more detailed certification may be required "if the defense contests [an] issue, or you have a cantankerous technophobe for a judge.").

[68] FED R. EVID. 902(13) advisory committee's note to 2017 amendment.

For a technology such as blockchain, which may be unfamiliar to the judge, more detail may be needed.[69]

Prosecutors may consider drafting a hybrid certification meeting the requirements of Rule 902(11) and Rule 902(13), similar to the hybrid 902 certifications commonly used to authenticate records obtained from electronic communication services. Proponents of the evidence should also be mindful that certifications under Rule 902(11) or Rule 902(13) change the *manner* in which evidence can be authenticated, but not the *standards* for authentication; if the testimony of the certifying witness would be insufficient to authenticate the records, the defect is not cured by presenting a certification rather than live testimony.[70] While proper certifications should not present Confrontation Clause issues, the matter is discussed in Section III.C., *infra*.

3. Judicial notice

A court may also take judicial notice of the blockchain pursuant to Rule 201. Courts have broad discretion to take judicial notice of evidence that, like the blockchain, can be "accurately and readily determined from sources whose accuracy cannot reasonably be questioned."[71] Courts have taken judicial notice of facts produced by an electronic process, including, notably, GPS data,[72] Google Maps,[73]

---

[69] Levy & Haried, *supra* note 49, at 84 ("The more familiar the technology is to the judge (and jury), the more likely a simple certification will suffice.").
[70] Grimm, *supra* note 61, at *1 ("These new amendments do not change the *standards* for authentication of electronic evidence. Rather, they change the *manner* in which the proponent's submission on authenticity can be made. Instead of calling a witness, the proponent can provide a certificate prepared by the witness of the submission that he would have made if required to testify. Of course, if that submission would be insufficient if he *had* testified, these new amendments will be of no use. An insufficient showing of authenticity does not somehow become better by way of a certificate in lieu of testimony.").
[71] FED R. EVID. 201.
[72] United States v. Brooks, 715 F.3d 1069 (8th Cir. 2013) (taking judicial notice of the accuracy and reliability of GPS technology in admitting GPS data obtained from a tracker placed in an envelope of stolen money in a bank robbery prosecution).
[73] *See, e.g.*, United States v. Burroughs, 810 F.3d 833, 835 n.1 (D.C. Cir. 2016) (Taking judicial notice of a Google Map, because, "It is a 'source[] whose accuracy cannot reasonably be questioned,' at least for the purpose of

and time and date information.[74] One court, finding the record deficient, even conducted its own research and took judicial notice that a "tack" marking coordinates on a Google Map was automatically generated, not manually placed and labeled.[75]

In requesting a court take judicial notice of blockchain records, a party should be prepared to provide the court with sufficient information to determine that the blockchain source's "accuracy cannot reasonably be questioned."[76] The background information on the blockchain in Section I., *supra*, and the references to the blockchain as the ground truth of virtual currency transactions in Section III.A., *supra*, may be useful for this purpose. Failure to provide the court with sufficient evidence regarding the blockchain's reliability may prevent the court from taking judicial notice of the blockchain's authenticity.[77]

---

identifying the area where [the defendant] was arrested and the general layout of the block."); McCormack v. Hiedeman, 694 F.3d 1004, 1008 n.1 (9th Cir. 2012) (relying on Google Maps to determine the distance between two locations because Google Maps' accuracy could not reasonably be questioned under Rule 201).

[74] Cline v. City of Mansfield, 745 F. Supp. 2d 773, 801 n.23 (N.D. Ohio 2010) (taking judicial notice that the sun set at a particular time on a particular day based on the information available at www.timeanddate.com).

[75] United States v. Lizarraga-Tirado, 789 F.3d 1107, 1108 (9th Cir. 2015).

[76] FED. R. EVID. 201.

[77] *See, e.g.,* Report and Recommendation, at *12–*13, Hunichen v. Atonomi LLC, 19-cv-00615, 2020 WL 1929372 (W.D. Wash., Oct. 6, 2020), ECF No. 126 (In deciding a Rule 12(b)(6) motion, declining to take judicial notice of several pieces of evidence, including blockchain records, because "Counter-defendants fail to support the proper consideration of the blockchain evidence through judicial notice or the doctrine of incorporation-by-reference. Specifically, the court is not persuaded the blockchain evidence is necessarily complete, its contents not subject to reasonable dispute or varying interpretation, and its use not improper as a defense to otherwise cognizable . . . ." The *Atonomi* court noted that, while Rule 201 permits the court to take judicial notice of a fact "not subject to reasonable dispute," FED R. EVID. 201(b), it does not permit the court to "take judicial notice of facts favorable to the moving party that could be reasonably disputed" and the opposing party in *Atonomi* did in fact dispute certain facts related to the blockchain evidence.) (internal citations omitted); *see generally* United States v. Kane, No. 2:13-cr-250, 2013 WL 5797619, at *9 (D. Nev. Oct. 28, 2013) (Expressing caution in taking judicial notice of websites because "the internet

Judicial notice of the blockchain will generally be limited to the authentication of the blockchain itself. Judicial notice does not relieve the government of its burden to explain the relevant activity or transactions on the blockchain.[78] The government will still need to provide evidence regarding those transactions to the jury, including, where relevant, evidence indicating the defendant—or some other party—was responsible for the transaction. Judicial notice simply avoids unnecessary authentication witnesses or bolsters the grounds for authentication of the blockchain evidence.

B. Overcoming hearsay concerns

The rule against hearsay prohibits the admission of an out-of-court statement "to prove the truth of the matter asserted."[79] Some legal commentators have raised concerns that courts could consider blockchain evidence inadmissible on hearsay grounds.[80] Any hearsay challenges to the admissibility of the blockchain can be readily overcome, however.[81] First, the blockchain records are not statements at all—they are electronically generated records. Second, even if the

---

contains an unlimited supply of information with varying degrees of reliability, permanence, and accessibility.") (citing Pickett v. Sheridan Health Care Center, 664 F.3d 632, 648 (7th Cir. 2011)).

[78] *See generally* Wilbon v. Plovanich, No. 12 C 1132, 2016 WL 890671, at *31–*32 (N.D. Ill. Mar. 9, 2016) (declining to take judicial notice of a Google Map because the proponent marked the map with a description of the defendant's alleged route).

[79] FED. R. EVID. 801(c)(2), 802.

[80] James Ching, *Is Blockchain Evidence Inadmissible Hearsay?*, LAW.COM (Jan. 7, 2016) ("[T]here is a potential hearsay barrier to the introduction of any result from a distributed ledger, permisionless [sic] or not and proprietary or not."); *see also* Casey C. Sullivan, *Could Blockchain Evidence Be Inadmissible?*, FINDLAW (May 5, 2016) (Summarizing Ching's arguments and noting, "It's possible that blockchain evidence may be inadmissible hearsay."); Emily Knight, *Blockchain Jenga: The Challenges of Blockchain Discovery and Admissibility Under the Federal Rule*s, 48 HOFSTRA L. REV. VOL. 519 ("The most notable question surrounding the admissibility of blockchain evidence is if the record constitutes admissible hearsay.").

[81] *Contra* Spring, *supra* note 38, at 935 ("[B]lockchain evidence is almost always inadmissible in federal court, and is only admissible under limited, factually specific scenarios. However . . . this state of affairs contradicts the very purpose of hearsay doctrine.").

blockchain records were statements, they would readily fall into one of several hearsay exceptions.

1. Not hearsay: electronically generated

As a threshold matter, records on the blockchain are not hearsay because the blockchain is electronically generated through automated processes.[82] For the purposes of the hearsay rules, a statement is defined as "a person's oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion."[83] Courts have widely held that machine-generated evidence is not hearsay.[84] As the court mused in *United States v. Moon*, "If [machine-produced readings] are 'statements' by a 'witness against' the defendants, then the machine must be the declarant. Yet how could one cross-examine a gas chromatograph? Producing spectographs, ovens, and centrifuges in court would serve no one's interests."[85]

---

[82] *See* Guo, *supra* note 38, at 446–47 ("Since humans do not actually generate the receipts on the blockchain, it is possible that courts will recognize distributed ledger receipts as computer-generated evidence and therefore not hearsay. Although people certainly engage directly in transferring Bitcoin to each other, records of each transaction are generated without human influence, entered automatically through a constantly-updating algorithm on every computer in the blockchain network."); Knight, *supra* note 80, at 519 ("With regard to a blockchain, courts may consider blockchain evidence to be solely computer-generated and not an assertion for the purposes of hearsay. In spite of the fact that people interact with the protocol in order to engage in a transaction, the *actual* record of the transaction, that is, the information contained in the block, is computer generated."); Justin Steffen, et al, *Lessons From A Crypto Mock Trial* (Feb. 22, 2019), https://www.icemiller.com/MediaLibraries/icemiller.com/IceMiller/PDFs/3-Lessons-From-A-Crypto-Mock-Trial.pdf (Describing the admission of blockchain evidence at a mock trial over a defense hearsay objection and noting, "Judge Blakey likened the record to a verbal or 'mechanical act' akin to the display of time on a clock, rather than an out-of-court statement.").

[83] FED. R. EVID. 801(a).

[84] *See* United States v. Lamons, 532 F.3d 1251, 1263 (11th Cir. 2008); United States v. Moon, 512 F.3d 359, 362 (7th Cir. 2008); United States v. Washington, 498 F.3d 225, 230 (4th Cir. 2007); United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005); United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003).

[85] *Moon,* 512 F.3d at 362.

Some writers have questioned whether the blockchain is appropriately treated as machine-generated given the involvement of humans in originating the transactions.[86] As the Eleventh Circuit noted in *United States v. Lamons*, "there can be no statements which are wholly machine-generated in the strictest sense; all machines were designed and built by humans."[87] Indeed, any review of the blockchain itself would confirm that the data contained therein does not resemble any human statement, even if a human-initiated transaction underlies the data. There is a reason that law enforcement uses blockchain analysis software rather than reviewing the blockchain data by hand in its raw form.

Existing case law supports this approach. Blockchain evidence is quite similar to the transaction records the Tenth Circuit deemed non-hearsay in *United States v. Channon*.[88] *Channon* involved Excel spreadsheets containing transaction records that were created at the point of sale, transferred to the merchant's servers, and then passed to a database maintained by another party. While these records were of transactions that people conducted at the merchant's stores, the *Channon* court conclusively found that "these records were produced by machines" and were not statements for hearsay purposes.

Other fact patterns considered by courts are similarly illustrative. The Third Circuit, for example, determined that fax headers were non-hearsay machine statements[89] even though that information was necessarily derived from a human who entered the information routing the fax. Indeed, in finding the district court's decision to exclude the evidence harmless, the Third Circuit observed, "Fax

---

[86] *See* Guo, *supra* note 38, at 446–47 ("Since each transaction recorded in a distributed ledger is the direct result of human transaction—and is cryptographically signed by the "owner" of Bitcoin wallet with his private key—the amount of influence that a person has on such a machine-made assertion is arguably much larger than any possible impact someone could have on a digital photograph."); Knight, *supra* note 80, at 519 ("Given the fact that records of blockchain transactions result from human activity of, at the very least, initializing the transaction, one can opine that there is a greater amount of human impact over the machine-made blockchain record compared with the level of influence over a digital photograph.").

[87] *Lamons*, 532 F.3d at 1263 n.23.

[88] United States v. Channon, 881 F.3d 806, 811 (10th Cir. 2018).

[89] *Khorozian*, 333 F.3d at 506.

headers are easily fabricated by the sender."[90] The Eleventh Circuit determined that a data compilation of telephone calls, showing calls originating from the defendant's cell phone number, was similarly non-hearsay, despite the role of persons in initiating and receiving the calls.[91] As these cases make clear, the involvement of humans in activity giving rise to the computer-generated records does not transform the records themselves into hearsay statements.

2. Business record

Rule 803(6) permits the admission of records of regularly conducted activity as an exception to the general bar of hearsay evidence. Rule 803(6), commonly referred to as the business record exception, allows for the admission of "a record of an act, event, condition, opinion, or diagnosis" if three conditions are met: (1) "the record was made at or near the time by—or from information transmitted by—someone with knowledge;" (2) "the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;" and (3) "making the record was a regular practice of that activity."[92] The blockchain readily meets each condition.

The discussion categorizing blockchain evidence as a business record is discussed in Section III.A., *supra*. That discussion dealt with the use of a business record certification pursuant to 902(11) to authenticate blockchain evidence—which is distinct from the requirement that, once authenticated, the evidence must still be categorized as non-hearsay or fall within an exception in order to be admitted. The analysis of the categorization of the blockchain evidence as a business record is largely transferrable, however, since Rule 902(11) incorporates Rule 803(6).

3. Market report

Blockchain evidence may also fall into the hearsay exception set forth in Rule 803(17), *market reports and similar commercial publications*, which excepts "[m]arket quotations, lists, directories, or other compilations that are generally relied on by the public or by

---

[90] *Id*. at 507.

[91] *Lamons,* 532 F.3d at 1263 ("We have no difficulty concluding that the statements in question are the statements of machines, not statements of persons.").

[92] FED. R. EVID. 803(6).

persons in particular occupations."[93] Weinstein's Federal Evidence explains:

> As with other hearsay exceptions, the admissibility of market reports and commercial publications under Rule 803(17) is predicated on the two factors of necessity and reliability. Necessity lies in the fact that if this evidence is to be obtained it must come from the compilation, since the task of finding every person who had a hand in making the report or list would be impossible. Reliability is assured because the compilers know that their work will be consulted; if it is inaccurate, the public or the trade will cease consulting their product.[94]

Courts have found that the Kelley Blue Book, a New York Stock Exchange (NYSE) Trade & Bid database, a report compiling a list patents that was created by a consulting firm, a CARFAX history report, Bloomberg Market Reports, a database maintained by the National Insurance Crime Bureau (NICB), a real estate database, and LexisNexis all fall within the Rule 803(17) exception.[95]

---

[93] FED. R. EVID. 803(17).

[94] JACK B. WEINSTEIN & MARGARET A. BERGER, 5 WEINSTEIN'S FEDERAL EVIDENCE § 803.19 (2021).

[95] *In re* Penny, No. 10-55073, 2011 WL 20488, at *6 (Bankr. N.D. Cal. Jan. 21, 2011) (Determining that the Kelley Blue Book is covered by Rule 803(13), noting, "The Kelley Blue Book is objective, serves the interests of standardization and predictability, and is cost-effective, which benefits the parties."); Sec. Exch. Comm'n v. Competitive Techs., Inc., No. 3:04-cv-1331, 2006 WL 3346210, at *8 (D. Conn. Nov. 6, 2006) (NYSE Trade & Bid database); *In re* Innovatio IP Ventures, LLC, Pat. Litig., No. 11 C 9308, 2013 WL 5393609, at *177 (N.D. Ill. Oct. 3, 2013) (list of patients created by a consulting firm); Garcia v. Roy's Trucks & Equip., No. 17-CV-0950, 2018 WL 6338364, at *5 (N.D. Tex. Aug. 24, 2018) (CARFAX); *see* United States v. Masferrer, 514 F.3d 1158, 1162 (11th Cir. 2008) ("The government presented evidence at trial establishing that Bloomberg financial information is universally relied upon by individuals and institutions involved in financial markets."); United States v. Goudy, 792 F.2d 664, 674 (7th Cir. 1986) (admitting a bank directory showing the "routing number" prefix for Los Angeles); United States v. Olson, No. 94-30387, 1995 WL 746177, at *1 (9th Cir. 1995) (admitting a "Gun Trader's Guide" that indicated where a firearm was manufactured); United States v. Cassiere, 4 F.3d 1006 (1st Cir.

4. Residual exception

Even if blockchain evidence does not fall into one of the above hearsay exceptions, it is a prime candidate for inclusion under the residual hearsay exception.[96] The residual hearsay exception, set forth in Rule 807, was revised in December 2019. Under Rule 807, a hearsay statement should not be not excluded, even if it does not fall into a defined hearsay exception, if the statement is "supported by sufficient guarantees of trustworthiness" and is "more probative on the point for which it is offered" than any other evidence that can be

---

1993) (admitting the publication "County Comps," which contained data regarding the monthly listings of properties sold, the sales prices, and the dates the sales were closed); United States v. Woods, 321 F.3d 361, 364 (3d Cir. 2003) ("Because we are satisfied that the NICB database is both necessary and reliable, we conclude that it is precisely the type of evidence that Rule 803(17) envisions."); U.S. Bank, Nat'l Ass'n v. UBS Real Estate Sec. Inc., 205 F. Supp. 3d 386, 442 (S.D.N.Y. 2016) (real estate database and LexisNexis) (Determining that a "database that includes information on properties by owner and transaction history" was appropriately admitted under 803(17) where the witness "testified that he and other underwriters and re-underwriters commonly used the database as a source of information.") (Determining that records from LexisNexis were appropriately admitted under 803(17) where the witness testified that LexisNexis "provides a lot of information" to help identify fraud, and is commonly used by underwriters to identify fraud."). *But see* In re C.R. Bard, Inc., 810 F.3d 913, 924 (4th Cir. 2016) (A Material Data Safety Sheet (MSDS) was not appropriately admitted under 803(17) where a party "sought to use a portion of the MSDS that was not factual but rather operated as a warning and disclaimer of liability for the self-interested issuing party. The warning from Phillips that polypropylene should not be used in human implants was an opinion the company issued within the MSDS for self-interested reasons, and it therefore bears no resemblance to the factual, list-type documents enumerated in Rule 803(17)."); Shepherd v. Am. Broad. Cos., 862 F. Supp. 505, 508 n.13 (D.D.C. 1994) (Rejecting the argument that legal fee surveys published in the *Legal Times* were admissible under 803(17) because, "The court is not yet convinced that published fee surveys reliably reflect rates actually billed and not rates that surveyed lawyers have artificially inflated for the *Legal Times* audience.").

[96] *C.f.* Spring, *supra* note 38, at 944 ("[W]hile the residual exception is currently the best method to admit blockchain evidence, on policy grounds, it is not a particularly good one," instead proposing an amendment to the Federal Rules of Evidence to allow for the admission of blockchain evidence.).

reasonably obtained.[97] In assessing the guarantees of trustworthiness, the court should consider any corroborating evidence as well as "the totality of circumstances" in which the statement was made.

The residual exception should be used only where a hearsay statement cannot be admitted under another exception.[98] Since blockchain evidence should not be considered hearsay at all, and even if it were, it would fall into one of several exceptions discussed *supra*, prosecutors will rarely need to invoke the residual exception. It is, however, available as a lifeline if needed.

5. Specific transactions may fall outside of hearsay preclusion

Even if a court were to find that transactions are statements that do not fall into one of the above exceptions, specific transactions would be admissible. If transactions are statements, then transactions conducted by the defendant would be admissible as statements of a party opponent. Transactions conducted by co-conspirators as part of the criminal scheme would similarly be admissible. Victims, undercover agents, or other transaction counterparties could testify to their own transactions.

C. Confrontation Clause issues

The Confrontation Clause of the Sixth Amendment generally bars the admission of testimonial hearsay in a criminal case where there is no opportunity for cross-examination.[99] A statement is considered testimonial for Sixth Amendment analysis when its "primary purpose . . . is to establish or prove past events potentially relevant to later criminal prosecution."[100]

---

[97] FED. R. EVID. 807.

[98] FED. R. EVID. 807 advisory committee's notes to 2019 amendment ("[T]he opponent cannot seek admission under Rule 807 if it is apparent that the hearsay could be admitted under another exception."). *Contra id.* ("A court is not required to make a finding that no other hearsay exception is applicable.").

[99] Crawford v. Washington, 541 U.S. 36, 59 (2004) ("Testimonial statements of witnesses absent from trial have been admitted only where the declarant is unavailable, and only where the defendant has had a prior opportunity to cross-examine.").

[100] Davis v. Washington, 547 U.S. 813 (2006).

This generally will not pose an issue for blockchain evidence because, as discussed *infra*, the records are not hearsay because they are machine generated; and even if they were hearsay, they would be non-testimonial as business records and not created in anticipation of litigation.[101]

As the Eleventh Circuit observed in *United States v. Lamons*, "the witnesses with whom the Confrontation Clause is concerned are *human* witnesses."[102] As Judge Grimm, a renowned electronic evidence expert and jurist, noted, "while [a] machine output might be prepared for litigation, *it is not testimonial because it is not hearsay*. Machines do not make statements, and cannot be cross-examined; and the Confrontation Clause applies only to statements that are hearsay."[103] Additionally, as the Supreme Court noted in *Crawford v. Washington*, certain categories of hearsay exceptions, including business records, are non-testimonial by their nature.[104]

If the government uses certifications under Rule 902 to authenticate the evidence, prosecutors should be mindful of the manner in which the certifications are drafted and their treatment in court to avoid any Confrontation Clause issues. A more fulsome discussion of Confrontation Clause considerations specific to electronic evidence certifications is included in *Authenticating Digital Evidence* within the February 2019 edition of this publication.[105] Courts are primarily concerned with Confrontation Clause issues arising from certifications of data where the data itself—not just the certificate attesting to the

---

[101] *C.f.* Guo, *supra* note 38, at 444–45 ("[B[lockchain evidence, as an out-of-court 'assertion' utilized to prove the truth of the matter, would probably be subject to both hearsay scrutiny and possibly Confrontation Clause analysis.") (citing U.S. v. Lizarraga-Tirado, 789 F.3d 1107, 1110 (9th Cir. 2015)); *Id.* at *13 n 1.

[102] United States v. Lamons, 532 F.3d 1251, 1263 (11th Cir. 2008).

[103] Grimm, *supra* note 61, at 49.

[104] *Crawford*, 541 U.S. at 56; *see also* Tran v. Roden, 847 F.3d 44, 51 (1st Cir. 2017) ("[B]usiness records [are not] testimonial as long as they are not created for the purpose of prosecution.") United States v. Forty-Febres, No. 16-330, 2018 WL 2182653, at *6–*7 (D.P.R. May 11, 2018) ("The registration records at issue are non-testimonial business records that were not created for the purpose of prosecution, but created in the ordinary course of DTOP's business.").

[105] Levy & Haried, *supra* note 49, at 86–93.

data's authenticity—was created for use at trial.[106] Because the blockchain records themselves—albeit not the certifications—were created before and apart from litigation, they generally will not raise Confrontation Clause issues.[107] And where the certification is not presented to the jury but instead is used to satisfy a judge's criteria for admission before introducing the records through the testimony of a live witness, no Confrontation Clause issues arise.[108]

D. Presenting the trial testimony

In considering trial testimony involving blockchain evidence, prosecutors are advised to consider *what* evidence to present, *who* to present the evidence through, and *how* to present it.

1. What to present

Prosecutors should think carefully about exactly what evidence they need to present to the jury and how they can streamline or simplify that presentation. Case teams often default to telling the story based on how the investigation developed chronologically, but this is frequently not the most effective approach for trial presentation.

In many instances, prosecutors will not have to rely on the blockchain at all when presenting evidence in a virtual currency case. Prosecutors may be able to tell a compelling story based on business records from virtual currency exchanges, testimony of victims, or electronic evidence recovered from defendant's devices or online accounts. For example, in *United States v. Brown*, where the

---

[106] Melendez-Diaz v. Massachusetts, 557 U.S. 305, 322–23 (2009) (recognizing that a custodian "could by affidavit *authenticate* or provide a copy of an otherwise admissible record, but could not . . . *create* a record for the sole purpose of providing evidence against a defendant").

[107] Grimm, *supra* note 61, at 50 ("So at the very least, Rule 902(13) certifications would . . . be properly admitted in the large number of situations in which the authenticated information was generated before the litigation arose.").

[108] *See id.* at 50–51 & n.143 ("The government may well opt to use the certificate to pass the admissibility threshold with the judge, and then establish its authenticity to the jury (if challenged, as it often is not) by way of a witness, who will likely provide a more interesting presentation than a certificate ever could. When the government makes that decision, the certificate raises no constitutional concerns because it is not admitted at trial and so the declarant is not a "witness against" the defendant.").

defendant attempted to extort a victim for a demand in bitcoin, the government introduced evidence of the ransom demand listing a specific Bitcoin address and introduced internet history evidence recovered from the defendant's computer showing that he checked that address' balance on a popular open-source blockchain explorer.[109] This was significant because the address was previously unused and, therefore, should have been known only to the perpetrator and the recipient of the ransom demand. Coupled with additional testimony providing this background and context for the uniqueness of a bitcoin address, this evidence would allow a jury to understand the significance of the defendant's interest in the ransom address separate from any blockchain-based presentation. Prosecutors should consider whether admitting records from the blockchain itself is truly necessary.

Often, cases that involved extremely complex blockchain analysis in the investigative stage can be told in a much simpler fashion by the time the case arrives at trial. Consider, for example, a 2017–2018 investigation into a website selling access to child exploitation material and accepting payment in bitcoin. Using blockchain analytics software, law enforcement identified the cluster of bitcoin addresses associated with the website.[110] Law enforcement further noted transactions sent to the website from Coinbase, a U.S.-based virtual currency exchange.[111] Using that cluster analysis, law enforcement sent a subpoena to Coinbase, which produced customer information that allowed law enforcement to identify individuals buying child exploitation material on the site.[112] Several months later, law enforcement seized the servers hosting the website.[113] A forensic review of those servers revealed the same bitcoin addresses contained

---

[109] Transcript at 98, United States v. Brown, 13-cr-118 (M. D. Tenn. May 10, 2016), ECF No. 177.

[110] Decl. Daniels in Support of Opp. Mtn. to Suppress at 6, United States v. Jung, No. 18-cr-00482 (N.D. Cal. June 4, 2019), ECF No. 30; Decl. Meyer in Support of Opp. Mtn. to Suppress at 3, United States v. Jung, No. 3:18-cr-00482, (N.D. Cal. June 4, 2019), ECF No. 29.

[111] Decl. Meyer in Support of Opp. Mtn. to Suppress at 4, United States v. Jung, No. 18-cr-00482, (N.D. Cal. June 4, 2019), ECF No. 29.

[112] *Id*. at 3.

[113] *Id*.

in the cluster from the earlier blockchain analysis.[114] Had this case gone to trial, the prosecutor could have bypassed explaining the details of cluster analysis entirely and, instead, simply introduced evidence of the bitcoin addresses found on the server when it was seized. Similarly, the prosecutor could have used the business records produced by Coinbase, which showed a transaction from the defendant's account to one of the bitcoin addresses located on the seized server,[115] rather than introduce the underlying blockchain evidence. In this way, the trial presentation could be quite straightforward, despite the more intricate process that led investigators to identify the defendant. Similar scenarios play out quite often in cases involving blockchain analysis, where a defendant initially may be identified in part through blockchain analysis, but a search of his electronic devices or accounts may provide alternative sources of evidence that obviate the need to introduce and explain more complicated blockchain analysis to a jury.

2. Who to present

This article devotes considerable attention to the grounds for admitting blockchain information in a self-authenticating form.[116] In practice, though, parties offering blockchain-related evidence at trial will want a witness to explain to the jury the fundamentals of virtual currency and blockchain analysis. This allows a jury to better understand the evidence and its context.

For a short trial with straightforward evidence, prosecutors may opt to introduce everything through the case agent. Even when the evidence is more complicated and involved, a case agent who is well versed in virtual currency may be highly effective in explaining the relevant concepts to the jury. For example, in *United States v. Ulbricht*, the trial of the administrator of the Silk Road darknet marketplace, one of the case agents explained the fundamentals of bitcoin, the blockchain, private keys, and addresses, among other

---

[114] *Id.* ("[T]he bitcoin addresses on The Website server itself—obtained separately and apart from the Reactor blockchain analysis—showed the same Bitcoin addresses found in The Website Cluster created by the cluster blockchain analysis.").

[115] *Id.*

[116] *See* Section III, *supra.*

concepts.[117] Similarly, in *United States v. Costanza*—a money laundering case involving a peer-to-peer virtual currency exchanger converting narcotics proceeds—the government introduced testimony regarding bitcoin and blockchain analysis through a member of the case team.[118] The detective, who had been involved in numerous virtual currency investigations and received training on blockchain analysis, testified about the fundamentals of blockchain analysis, as well as the details of his own undercover transactions with the defendant, which were represented to be the proceeds of narcotics sales.[119]

In other instances, prosecutors may choose instead to offer testimony through a law enforcement witness who was not part of the case team. This can be particularly useful if your case agent is not as experienced with the nuances of the technology underlying virtual currency. Being a highly effective investigator is often a different skill set than being able to explain technically complicated matters to a lay jury. Most major federal law enforcement agencies have individuals whose primary work portfolio centers on virtual currencies. These individuals work extensively on virtual currency matters and often deliver internal and external trainings and presentations on virtual currency. As a result, they are particularly well equipped to explain virtual currency and the blockchain to a lay jury.[120]

In some cases, parties may opt to bring in an individual from outside of the government to explain virtual currency and the blockchain. This individual may be sourced from, *inter alia*, academia, think tanks, consulting firms, policy-making groups, a private sector bitcoin company, or even just a virtual currency enthusiast.[121] This may be

---

[117] Transcript at 1661–63, United States v. Ross Ulbricht, 14-cr-68 (S.D.N.Y. Jan. 29, 2015), ECF No. 212.

[118] Transcript at 599, United States v. Costanzo, 17-cr-585, 2018 WL 11027104 (D. Ariz. Aug. 10, 2018), ECF No. 199.

[119] *Id.*

[120] *Id.* at 600 (providing an explanation of blockchain analysis by a member of the case team who presented briefings and presentations on virtual currency).

[121] *See generally* Guo, *supra* note 38, at 448 ("[A]n exchange programmer, an avid Bitcoin user, a programmer attempting to replicate the blockchain, a digital currency expert, or an investor could all be brought in at trial to explain the process, accuracy, and the exceptional reliability of blockchain receipts."), Knight, *supra* note 80, at 551 ("[A] litigant will have to offer

particularly helpful if the testimony does not pertain to a common virtual currency, such as Bitcoin, Ether, or Tether, but rather a more niche virtual currency with particular attributes that have significance to the investigation and may be best explained by someone particularly well versed in the nuances of that technology.

The choice to have the "Blockchain 101" testimony delivered through a law enforcement witness versus a private individual is one of general trial strategy and subject to varying opinions. Some prosecutors may prefer to open with a government witness who conveys a sense of knowledge and authority to the jury. The government is portrayed as in control and possessing the requisite knowledge and understanding to effectively investigate a serious crime.[122] Others may prefer instead to present the information through a "neutral" third party, whose lack of affiliation with the government may augment the perceived trustworthiness of the information.

Practice may differ by district as to whether the witness providing testimony regarding bitcoin and the blockchain needs to be noticed as an expert. This will also vary depending on whether a prosecutor is introducing the evidence through a case agent's testimony, interspersed among case-specific details, or through a separate witness specifically intended to explain virtual currency, the blockchain, clustering, or other details. The specific areas of testimony may ultimately be dispositive. In the Silk Road trial, for example, the government did not notice its government witnesses as experts. Instead, it used them to provide testimony about Bitcoin transactions, wallets, accounts, exchanges, and the blockchain, all concepts that the government noted were "familiar to any layperson who has ever used Bitcoins."[123] Similarly, the government, in *Costanzo,* introduced testimony regarding bitcoin, the blockchain, and virtual currency exchanges through a detective and an IRS agent who were not noticed

---

admissible proof of the accuracy of blockchain data in order to establish the records accuracy. This can be done by hiring an expert . . . .").

[122] *See, e.g.,* Transcript, United States v. Ulbricht, No. 14-cr-68 (S.D.N.Y. Jan. 13–15, 2015), ECF Nos. 196, 198, & 200 (A case agent testified for three days, explaining Bitcoin, the blockchain, Tor, and other concepts to the jury in addition to their relevance to the case itself.).

[123] Motion to Exclude Testimony at 5, United States v. Ulbricht, No. 14-cr-68 (S.D.N.Y. Jan. 29, 2015), ECF No. 165.

as experts.[124] While many prosecutors notice experts only where they are providing opinion testimony, there is no such restriction in Rule 702, which states that experts may testify "in the form of an opinion *or otherwise*."[125] Noticing an expert may be particularly useful when presenting clustering evidence, discussed further below in Section III.D., *infra*.

3. How to present it

Blockchain evidence can easily seem unnecessarily convoluted to even the most experienced prosecutors and agents, much less lay juries. A successful presentation to the jury will thus often necessitate distilling more complex information into more readily digestible exhibits.

In explaining the basics of virtual currency and the blockchain to the jury, parties are advised to make liberal use of demonstratives, to the extent the court will permit. Visual aids can greatly aid the jury in understanding the technical concepts presented. For example, the government, in *Silk Road*, displayed a diagram depicting a bitcoin transaction—using the iconic *Alice* and *Bob* participants—while having the case agent walk through the steps in a bitcoin transaction.[126] Careful selection of demonstrative exhibits can assist the trier of fact. Parties should be mindful when choosing demonstratives, however, to avoid those whose technical detail could confuse rather than clarify.

---

[124] Transcript at 611, United States v. Costanzo, 17-cr-585, 2018 WL 11027104 (D. Ariz. Aug. 10, 2018), ECF No. 199. The government in *Costanzo* did notice another IRS agent as an expert to testify about applicable financial regulations.

[125] FED. R. EVID. 702 (emphasis added); *see also* FED. R. EVID. 702 advisory committee's notes to proposed rules ("Most of the literature assumes that experts testify only in the form of opinions. The assumption is logically unfounded. The rule accordingly recognizes that an expert on the stand may give a dissertation or exposition of scientific or other principles relevant to the case, leaving the trier of fact to apply them to the facts."); Levy & Haried, *supra* note 49, at 93 ("Expert Witnesses do not have to testify in the form of opinion.").

[126] Transcript at 171, United States v. Ulbricht, 14-cr-68 (S.D.N.Y. Jan. 14, 2015), ECF No. 198.

Blockchain evidence is a perfect candidate for a summary exhibit, governed by Rule 1006 of the Federal Rules of Evidence.[127] The voluminous nature of the blockchain—over 300 GB[128] and encompassing over 580 million transactions[129]—makes it the exact sort of dataset envisioned by Rule 1006. Link charts showing the flow of funds will likely be among the most useful summary exhibits in the blockchain context. For example, a link chart consistent with Rule 1006 could depict the flow of funds from an undercover's wallet to the defendant's account at a virtual currency exchange, or any other sort of transaction path that is of relevance to the prosecution. Summary charts could also include spreadsheet-style charts summarizing the defendant's blockchain activity, such as the volume and value of transactions with various counterparties. These summaries will be much more useful to the jury in understanding the blockchain evidence than the raw presentation of hundreds or thousands of individual transactions.

4. Cluster-specific considerations

Many commercial blockchain analysis tools go beyond simply clustering addresses together and provide insight into who owns or controls key clusters associated with major services. For example, in most tools, the clusters associated with particular bitcoin exchanges are labeled and attributed to those exchanges. This information is not contained within the blockchain itself. Rather, the blockchain analysis software supplements the actual blockchain data with additional analysis or data sources to be able to say that *Cluster X* is, in fact, owned by *Bitcoin Exchange Y*. This information may come from the exchange itself, from open source information, or from the blockchain analysis firm conducting transactions with the exchange.

In the case of a Bitcoin exchange, replicating this attribution in a format easily presented in court is straightforward—a subpoena to the exchange will also show that the address of interest is held by that

---

[127] FED. R. EVID. 1006 ("The proponent may use a summary, chart, or calculation to prove the content of voluminous writings, recordings, or photographs that cannot be conveniently examined in court.").
[128] *Blockchain Size (MB)*, BLOCKCHAIN.COM (Nov. 1, 2020), https://www.blockchain.com/charts/blocks-size.
[129] *Total Number of Transactions*, BLOCKCHAIN.COM, https://www.blockchain.com/charts/n-transactions-total (last visited Feb. 11, 2021).

exchange. Presenting this attribution in court, however, can be more complex for clusters that are associated with services that are not able or available to confirm their own addresses. Take, for example, a prosecution of a darknet vendor who was selling narcotics on a particular darknet market. Once the investigators knew one of the vendor's addresses (which we will assume was identified independently), they could use blockchain analysis to identify transactions between the cluster of addresses controlled by the vendor and a large cluster of addresses, *Cluster X*. The blockchain analysis tool used by the investigators would likely label *Cluster X* as owned by *Darknet Market X*. Though in order to show at trial that *Cluster X* is in fact owned by *Darknet Market X*, the government has to present evidence beyond that contained in the blockchain itself.

There are numerous ways that the government can accomplish this objective. If *Darknet Market X* was shut down, and its servers seized by law enforcement, a law enforcement witness involved in that operation may be able to testify that the addresses of interest were found on *Darknet Market X*'s servers.[130] Also, an agent who conducted undercover transactions on *Darknet Market X* would be able to testify that she funded an account at *Darknet Market X* by sending virtual currency to a particular address, and additional blockchain analysis could be presented to explain that that address was contained within the cluster that transacted with the defendant. Alternatively, prosecutors could seek to have the blockchain analysis company testify to the basis for the cluster, though such an approach is generally disfavored and discouraged by the companies themselves, both to protect the companies' trade secrets and to avoid a situation where the blockchain analysis companies are asked to field witnesses for every major virtual currency trial when a law enforcement witness would more than suffice.

Parties may also consider whether clustering evidence is best presented through an expert pursuant to Rule 702, discussed in Section III.D., *supra*. This provides for greater flexibility in witness selection, as the expert can base her testimony on data that she "has

---

[130] For example, a witness in the Silk Road trial who reviewed the site's servers testified that there were over 2 million unique bitcoin addresses found on servers seized during the takedown of the Silk Road Marketplace. Transcript at 1684–86, United States v. Ulbricht, 14-cr-68 (S.D.N.Y. Jan. 29, 2015), ECF No. 212.

been made aware of," in addition to those that she personally observed.[131] This data need not even be admissible, provided certain requirements are met.[132] Prosecutors seeking to provide expert testimony regarding clustering, however, should be prepared for a potential *Daubert* hearing.[133] Prosecutors should develop a plan to appropriately address any trade secret or law enforcement privilege issue in advance of the *Daubert* hearing.[134]

In practice, defendants may want to stipulate to the attribution of certain clusters. A witness testifying about a particular address being associated with a particular darknet market or other criminal service will necessarily provide a fair amount of detail as to the illicit dealings of that platform. As a trial strategy, many defendants want to avoid putting more evidence before the jury regarding the nefarious activity perpetrated by groups linked to the defendant. Such stipulation has the added benefit of saving trial witnesses, who may need to travel from out of district at considerable expense and whose testimony would add to the length of the trial. Similarly, in some cases, certifications under 902(13) or 902(14) can help streamline the presentation of evidence about cluster attribution.

E. Discovery

The existence of blockchain-related evidence does not change a prosecutor's substantive discovery obligations. There are, however, some specific issues that warrant additional attention from the prosecutor.

While producing discovery, prosecutors should consider the extent of the blockchain evidence they will seek to admit at trial. If the evidence is likely to be constrained to discrete transactions that were analyzed by the case team, discovery may be relatively straightforward. If,

---

[131] FED. R. EVID. 703.

[132] FED. R. EVID. 703 ("If experts in the particular field would reasonably rely on those kinds of facts or data in forming an opinion on the subject, they need not be admissible for the opinion to be admitted. But if the facts or data would otherwise be inadmissible, the proponent of the opinion may disclose them to the jury only if their probative value in helping the jury evaluate the opinion substantially outweighs their prejudicial effect.").

[133] *See* Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579 (1993).

[134] The particulars of preparing for a *Daubert* hearing are beyond the scope of this article, but additional useful resources are available. *See, e.g., Expert Witnesses*, 58 U.S. ATTY'S BULL., no. 1, 2010.

however, the team envisions needing to rely on or admit voluminous records and use extensive summary charts, additional attention may need to be given to ensuring that prosecutors make the underlying data available to defense counsel, and to the court if requested.[135] In some cases—particularly in cases where the absence of transactions is as relevant as the existence of others—it may be appropriate to offer to produce a copy of the blockchain itself, or make it available for defense counsel to review.[136] In practice, defense counsel is unlikely to want to receive a 300 GB file of publicly available information.[137]

As discussed in Section III.D., *supra*, investigators may produce various charts using blockchain analysis tools over the course of their investigation. Many of these tools use a tool-specific graph format that may not be compatible with other software; as a result, the graphs may not be viewable outside of the specific software used to create them.[138] Prosecutors should anticipate this issue and develop a plan for producing the information to defense counsel. Some defense counsel who litigate extensively in blockchain matters—or, more likely, the experts they hire—may purchase licenses for the same commercial blockchain analytics tools that law enforcement uses. This scenario will streamline discovery considerably as the prosecution team can simply produce the graphs in their native file formats. In most situations, however, the prosecution team will need to consider

---

[135] FED. R. EVID. 1006 ("The proponent [of a summary chart] must make the originals or duplicates available for examination or copying, or both, by other parties at a reasonable time and place."); Sec. Exch. Comm'n v. Competitive Techs., Inc., No. 3:04-cv-1331, 2006 WL 3346210, at *8 (D. Conn. Nov. 6, 2006)(noting that the SEC should have produced the New York Stock Exchange (NYSE) Trade & Bid Database database).

[136] FED. R. EVID. 1006 ("The proponent [of a summary chart] must make the originals or duplicates available for examination or copying, or both, by other parties at a reasonable time and place."); *Competitive Techs., Inc.*, No. 04-cv-1331, 2006 WL 3346210, at *8 (noting that the SEC should have produced the New York Stock Exchange (NYSE) Trade & Bid Database database).

[137] Knight, *supra* note 80, at 549 ("With public blockchains, there is a limited need for discovery as the information stored can be easily viewed and accessed by a party in need of the information for his cause of action. This can be done through querying a public blockchain for relevant information via an applicable website.").

[138] This problem is not unique to blockchain data. Increasingly, law enforcement must use specific software and tools to effectively review electronic evidence.

the best alternative means to comply with its discovery obligations while making the information available to the defense. For example, the case team may consider exporting the raw data from a graph as CSV files or spreadsheets and taking screen captures of the charts. This can be a labor-intensive undertaking, and advanced planning helps simplify the process to the extent possible.

IV. Conclusion

In sum, blockchain analysis is a powerful tool that can be effectively leveraged at practically any stage of an investigation. Prosecutors handling a wide range of different types of cases may find blockchain analysis useful in identifying meritorious targets, developing probable cause to jump start an investigation, and even in proving a defendant's guilt beyond a reasonable doubt. That said, admitting blockchain analysis evidence is necessary only in a subset of cases, and prosecutors are well advised to think ahead about the various legal and practical challenges and considerations they may face when incorporating this technique into their investigative plan.

About the Authors

C. Alden Pelker is a Senior Counsel in the Computer Crime and Intellectual Property Section, where she investigates and prosecutes complex cyber criminal schemes involving the illicit use of cryptocurrency.

Christopher B. Brown is an Assistant United States Attorney in the Fraud Section, Cyber Crime Unit of the United States Attorney's Office for the District of Columbia, where he has served since 2014. He previously worked in the Office's Asset Forfeiture and Money Laundering Section and Cyber Crime Section.

Rich Tucker spent 11 years as an Assistant United States Attorney at the U.S. Attorney's Office in the Eastern District of New York, where he served as Chief of the National Security & Cybercrime Section and Senior Litigation Counsel for Cybercrime Investigations and Prosecution. In January 2021, Rich joined the secure identity company CLEAR as Senior Vice President, Legal, Privacy & Regulatory.